УДК 343.9.01

Л. Л. Мельник
следователь по особо важным делам
главного следственного управления
Следственного комитета Республики Беларусь

ОТДЕЛЬНЫЕ АСПЕКТЫ ПОДГОТОВКИ К ПРОВЕДЕНИЮ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

В настоящее время информационные технологии широко используются при совершении многих видов преступлений. Особое внимание лиц, совершающих преступления, привлечено к информационным технологиям, связанным с использованием криптовалют, в том числе самой распространенной — биткоина. Этому обстоятельству способствует популярность данной криптовалюты. Так, по состоянию на 26.01.2020 г. капитализация биткоина достигла 153 млрд долларов США [1].

В ходе совершения преступлений с использованием криптовалют, последние могут являться как предметом преступления, так и средством его совершения. В ходе расследования таких дел зачастую возникают вопросы по выявлению следов, в которых отразилась информация об их использовании. Полагаем, что наиболее значимым следственным действием с точки зрения получения возможного объема информации об использовании криптовалют является осмотр места происшествия. Следует отметить, что главной особенностью места происшествия по преступлениям, совершенным с использованием криптовалют, является его двойственная природа, так как оно включает в себя как виртуальный, так и реальный мир. В связи со сложностью проведения вышеуказанного следственного действия, возможностью упустить значимые доказательства, которые уже впоследствии невозможно будет вновь получить, следует тщательно осуществлять подготовку к его проведению. В частности, важно точно определить круг задач, которые стоят перед следователем в конкретной следственной ситуации. При этом лицо, производящее осмотр, должно четко знать потенциальное местонахождение электронных и материальных следов криптовалюты. Представляется, что первоначально на примере наиболее распространенной криптовалюты биткоин необходимо описать типичные электронные и материальные

следы установки соответствующего программного обеспечения для ее использования, на которые следует обратить внимание при осмотре места происшествия.

Так, лицо, которое использует биткоин, может устанавливать программное обеспечение в любое место в памяти накопителя информации. При этом в случае выбора местоположения данного программного обеспечения по умолчанию его путь нахождения будет выглядеть следующим образом:

1) в операционной системе Windows XP: C:\Documents и Settings\<username>\Application data\Bitcoin; в операционных системах Windows (Vista, 7, 8, 10): C:\Users\<username>\Appdata\Roaming\Bitcoin;

2) на всех версиях операционной системы Mac OS X: ~/Library/Application Support/Bitcoin/;

3) в основных версиях операционной системы Linux: ~/.bitcoin/.

Следует отметить, что имеется различное программное обеспечение для использования биткоин-кошельков с помощью стационарных компьютеров, но самое популярное среди них — Bitcoin Core. Программное обеспечение Bitcoin Core требует загрузки истории всего блокчейна. Данное программное обеспечение создает файл wallet.dat на локальном диске компьютера. В указанном файле хранится закрытый ключ, который может быть как в незашифрованном виде, так и в зашифрованном. В случае если ключ зашифрован, то для его расшифровки необходима помощь владельца исследуемого кошелька. Также следует учитывать, что существуют «легкие» кошельки, или веб-кошельки, при создании которых не загружается полная история блокчейна. Самые популярные из них — Blockchain.com.

Для получения доступа к управлению биткоин-кошельком, например для наложения ареста на хранящиеся в нем биткоины, необходимо отыскать закрытый ключ управления, который содержится:

1) в файле wallet.dat на ЭВМ, телефоне или ином электронном носителе информации, включая аппаратный кошелек;

2) на бумаге в виде сгенерированного QR-кода или перезаписанных значений закрытых ключей;

3) на серверах виртуальной биржи или онлайн-провайдера кошелька.

Для доступа к веб-кошелькам требуется имя пользователя или ID кошелька, пароль и, возможно, код двухфакторной аутентификации.

Бумажные кошельки также пользуются популярностью, так как хранят закрытые ключи вне сети Интернет. В случае обнаружения бумаж-

ный кошелек позволит получить доступ к биткоинам, связанным с этим закрытым ключом.

Восстановление доступа к закрытому ключу может произойти также с использованием seed-фразы, которая представляет собой набор от 12 до 24 слов из специального словаря. Обнаружение следователем seed-фразы позволит ему получить доступ ко всем биткоин-адресам в кошельке.

В аппаратном кошельке, который представляет собой защищенное устройство, хранятся закрытые ключи пользователя. Такое устройство защищено от использования в отношении него вредоносного программного обеспечения или изъятия правоохранительными органами, следовательно, необходимо сотрудничество подозреваемого для доступа к средствам, хранящимся на аппаратном кошельке.

Биткоин-кошельки для мобильных телефонов существуют в наиболее популярных мобильных операционных системах — Android/IOS/Windows Phone. Эти биткоин-кошельки хранят личные ключи пользователя в приложении на телефоне.

Доступ к закрытым ключам для мобильных биткоин-кошельков требует разблокировки телефона, а также открытия приложения, которое может быть заблокировано с помощью проверки ПИН-кода/отпечатка пальца.

Таким образом, знание вышеуказанных возможных следов установки программного обеспечения с целью использования биткоинов позволит лицу, производящему осмотр места происшествия, правильно определить дальнейший ход расследования и пути взаимодействия с лицом, у которого данная криптовалюта находилась в пользовании.

Далее лицо, производящее осмотр места происшествия, должно выделить задачи, которые необходимо определить до начала осмотра места происшествия. Среди них следует выделить следующие:

- установить круг предполагаемых объектов, которые имеют значение по делу, подлежат поиску и последующему изъятию;
- определить возможные места хранения объектов, подлежащих обнаружению и изъятию;
- подготовить и проверить служебную технику и материалы, необходимые для проведения осмотра;
- установить сведения о наличии криптоконтейнеров, в том числе о наличии факта шифровки логических разделов предполагаемых к изъятию электронных устройств;

- получить сведения о паролях доступа к защищенным объектам хранения, которые содержат криминалистически важную информацию;

- с учетом выполнения вышеуказанных задач определить тактику проникновения в помещение (иное владение, где будет проводиться осмотр) с целью минимизации риска уничтожения или повреждения объектов, подлежащих изъятию.

Четкая постановка лицом, производящим осмотр места происшествия, перед собой круга задач, которые необходимо решить в ходе проведения осмотра места происшествия по преступлениям, совершенным с использованием криптовалюты, с учетом двойственной природы места происшествия способствует получению наиболее полного объема необходимой информации для последующего успешного расследования.

Список основных источников

1. Биткоин [Электронный ресурс]. — Режим доступа: https://coinmarketcap.com/ru/currencies/bitcoin. — Дата доступа: 26.01.2020. Вернуться к статье